Amendments to the Claims:

This listing of claims will replace all prior versions, and listings of claims in the application:

1.   (Original) A method for preventing unauthorized downloading of software into a diagnostic tool, comprising the steps of:

providing a first external storage device that is electrically coupled to the diagnostic tool, the first external storage device including a first security signature;

providing a second external storage device that is electrically coupled to the diagnostic tool, the second external storage device including software; and

downloading the software into an internal storage device of the diagnostic tool when a second security signature included within the diagnostic tool is the same as the first security signature included within the first external storage device.

2.   (Original) The method of claim 1, wherein the first external storage device is a smart card that provides the first security signature to the diagnostic tool through a smart card reader.

3.   (Original) The method of claim 1, wherein the second external storage device is electrically coupled to the diagnostic tool through a serial port.

4.   (Original) The method of claim 3, wherein the serial port is a USB port.

5.   (Original) The method of claim 3, wherein the serial port is a RS232 port.

6.   (Original) The method of claim 3, wherein the serial port is an IrDA compatible

infrared port.

7.   (Original) The method of claim 3, wherein the serial port is an IEEE 1394 port.

8.   (Original) The method of claim 1, further comprising the step of:

modifying the first security signature upon successful downloading of the software into

the internal storage device located within the diagnostic tool.

9.   (Original) The method of claim 8, wherein the first security signature is modified

so that it cannot be further utilized to download the software into any diagnostic tool.

10.   (Original) The method of claim 9, wherein the first security signature is erased.

11.   (Original) A diagnostic tool for communicating with a plurality of motor vehicle

control units, the diagnostic tool preventing the unauthorized downloading of software into the

diagnostic tool, the diagnostic tool comprising:

a processor for controlling the downloading of software into the diagnostic tool;

a first port for electrically coupling the processor to a first storage device, the first storage

device including a first security signature; and

a second port for electrically coupling the processor to a second storage device, the

second storage device including software, wherein the diagnostic tool downloads the software

into a third storage device located within the diagnostic tool when a second security signature

stored within the diagnostic tool is the same as the first security signature included within the

first storage device.

12.   (Original) The diagnostic tool of claim 11, wherein the first storage device is a

smart card that provides the first security signature to the diagnostic tool through a smart card

reader.

13.   (Original) The diagnostic tool of claim 11, wherein the second storage device is

electrically coupled to the diagnostic tool through a serial port.

14.   (Original) The diagnostic tool of claim 13, wherein the serial port is a USB port.

15.   (Original) The diagnostic tool of claim 13, wherein the serial port is a RS232

port.

16.   (Original) The diagnostic tool of claim 13, wherein the serial port is an IrDA

compatible infrared port.

17.   (Original) The diagnostic tool of claim 13, wherein the serial port is an IEEE

1394 port.

18.   (Original) The diagnostic tool of claim 11, wherein the processor causes the first security signature to be modified upon successful downloading of the software into the third storage device located within the diagnostic tool.

19.   (Original) The diagnostic tool of claim 18, wherein the first security signature is modified so that it cannot be further utilized to download the software into any diagnostic tool.

20.   (Original) The diagnostic tool of claim 19, wherein the first security signature is erased.

21.   (Original) The diagnostic tool of claim 11, wherein the first storage device is a smart card and the second storage device is a flash ROM.

22.   (Original) The diagnostic tool of claim 11, wherein the first storage device is a smart card and the second storage device is an EEPROM.

23.   (Original) The diagnostic tool of claim 11, further including:

a keypad coupled to the processor for receiving input from a user, the user initiating the downloading of the software by selecting a particular menu item from a list of menu items; and

a display coupled to the processor for providing the list of menu items to the user of the diagnostic tool.

24.   (Original) A method for preventing unauthorized downloading of software into a diagnostic tool, comprising the steps of:

providing an external storage device that is electrically coupled to the diagnostic tool, the external storage device including a first security signature and software; and

downloading the software into a memory of the diagnostic tool when a second security signature included within the diagnostic tool is the same as the first security signature included within the external storage device.

25.   (Original) The method of claim 24, further including the step of :

storing the second security signature of the diagnostic tool as the first security signature on the external storage device when the first security signature is determined to be a default value.

26.   (Original) The method of claim 24, wherein the external storage device is a flash ROM.

27.   (Original) A diagnostic tool for communicating with a plurality of motor vehicle control units, the diagnostic tool preventing the unauthorized downloading of software by the diagnostic tool, the diagnostic tool comprising:

a processor for executing the software;

a port for electrically coupling the processor to an external storage device, the external storage device including a first security signature and software, where the diagnostic tool downloads the software into a memory of the diagnostic tool when a second security signature

included within the diagnostic tool is the same as the first security signature included within the external storage device.

28.   (Original) The diagnostic tool of claim 27, wherein the processor causes the second security signature of the diagnostic tool to be stored as the first security signature on the external storage device when the first security signature is determined to be a default value.

29.   (Original) The diagnostic tool of claim 27, wherein the external storage device is a flash ROM.